AMERICAN TRUST: CONFIDENCE IN THE ABILITY OF THE UNITED STATES GOVERNMENT TO SUCCESSFULLY RESPOND TO ACTS OF CYBERTERRORISM

by
Michael Alan Sanders

A capstone submitted to Johns Hopkins University in conformity with the requirements for the degree of Master of Science in Government Analytics

Baltimore, Maryland
April 2018

Abstract

Determining the impact of cyberterrorism – a relatively recent construct – on individuals' trust in the United States government is an area of study lacking longitudinal research. Existing studies provide only topical analysis, leaving room for significant academic research into an emerging topic of substantial concern. This study aims to determine whether American citizens trust the United States government to respond to cyber attacks targeting government entities and public infrastructure, areas likely to be determined to be acts of cyberterrorism. The results from this study indicate that queried individuals' age, sex, political ideology, education, and employment statuses have a statistically significant impact on the respondents' overall trust in their government's ability to adequately respond to cyber attacks targeting both government and public entities and infrastructure.

Contents

1. Introduction

The United States is not immune to acts of terrorism. Perhaps most globally recognized are the events that unfolded on September 11, 2001, when terrorists hijacked four commercial airlines and flew them in to the World Trade Center towers, the Pentagon, and a third target that was unsuccessful due to the actions taken by passengers. On that day, nearly 3,000 people were killed, with many more that suffered long-term illnesses due to exposure to the debris. These attacks, coordinated by Al Qaeda, required years of planning and hinged on avoiding detection by a multi-tiered national security system.[1]

According to the United States' Department of State, terrorism is the "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[2] Title 22 of the United States Code, Section 2656 requires the Department of State to provide Congress with a full report of all global activities that meet this definition. Since 2007, there have been at least 111,757 acts of terrorism that have taken place around the globe, resulting in at least 195,131 deaths and 325,405 injuries.[3] Despite the brutality of these attacks, none were ever able to cause a direct impact to an entire nation in a single moment. At least until now.

This new threat is cyberterrorism, a modern technology-driven addition to existing conventional options for committing acts of terrorism. Rather than subnational groups or other clandestine agents, a single individual – with the right technical expertise

[1] "Final Report of the National Commission on Terrorist Attacks Upon the United States," (Washington, District of Columbia: National Commission on Terrorist Attacks Upon the United States, 2004).
[2] "Annex of Statistical Information: Country Reports on Terrorism 2016 ", (2017).
[3] "Country Reports on Terrorism," (United States Department of Justice, Multiple).

– can target a nation's critical infrastructure, potentially shutting down vital services such as electricity or water, without the geographical constraints associated with traditional acts of terrorism. But attacks need not reach this magnitude to impact the populace. Large-scale cyber campaigns targeting banks, hospitals, or other strategic public services can cause widespread fear among United States citizens, as well as result in loss of life.

This research studies surveyed individuals' trust in the United States government's ability to respond to cyber attacks targeting government entities and public infrastructure, the most likely targets during an act of cyberterrorism.

2. Literature Review and Theoretical Framework

For decades research has analyzed the psychological impact of terrorism on populations. However, much of this research has focused on acts of terrorism that conventionally involve a physical aspect to invoke terror in targeted masses. The threat landscapes terrorists can leverage have changed drastically from when much of this research took place, forcing researchers to consider a new and very unique form of terrorism, one that can impact an entire nation – or the entire world – without the proverbial shot ever needing to being fired: cyberterrorism.[4] Unfortunately, the body of academic literature covering the psychological effects of cyberterrorism has not reached the same level of study as that of conventional terrorism.

Compared to more contemporary schools of thought on what might constitute a "conventional" act of terrorism, the novelty of cyberterrorism creates discord among

[4] Michael L. Gross, Daphna Canetti, and Dana R. Vashdi, "The Psychological Effects of Cyber Terrorism," *Bulletin of the Atomic Scientists* 72, no. 5 (2016).

researchers and the general populace in terms of what it actually is.[5] [6] As far as actions traditionally referred to as acts of terrorism are concerned, there is often a physical component that accompanies and amplifies the psychological impact of such events.[7] The attacks on the World Trade Center in New York City on September 11, 2001 are a prime example. Through this attack, a known terrorist group sent America's citizens a clear ideological message; but without the tangible, violent medium in which it was delivered, it might have been impossible for this message to be received with the same impact and clarity. This attack had a direct and immediate impact on citizens, one that still resonates over 16 years later, precisely because of its impact on citizens' immediate surroundings, routines, and--for those victims of the attack--their duration life.[8] Unfortunately, however, it is difficult to say with absolute certainty that acts of terrorism truly require a tangible aspect as the key component is terror.

While attacks in the cyber realm of the magnitude of the September 11, 2001 attacks have yet to occur, the pace at which general cyber attacks transpire at other levels of society that have remained either totally or relatively unseen by the general populace, and the interweaving of technology into nearly every facet of daily life, is a sign of possible things to come. Cyber attacks have the capability to cause significant physical damage, although these have been more often reserved for state-sponsored levels of attacks, orchestrated by nation-states with strategic objectives in mind. To put the relative newness of the concept of cyberterrorism into perspective, the first known instance of a

---

[5] Thomas M. Chen and Lee Jarvis, *Cyberterrorism: Understanding, Assessment, and Response*, ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald (New York: Springer, 2014).
[6] Gross, Canetti, and Vashdi, "The Psychological Effects of Cyber Terrorism."
[7] Marc Rogers, "The Psychology of Cyber-Terrorism," in *Terrorists, Victims, and Society : Psychological Perspectives on Terrorism and Its Consequences*, ed. Andrew Silke, Wiley Series in the Psychology of Crime, Policing and Law (Chichester, West Sussex, England: Wiley, 2003).
[8] Itzhak Levav, "Terrorism and Its Effects on Mental Health," *World Psychology* 5, no. 1 (2006).

cyber attack that caused physical damage did not occur until January 2010 – that weapon became known globally as Stuxnet, a sophisticated piece of malware crafted by state-level agencies to target and degrade Iran's nuclear program.[9] Most existing studies focus predominately on cyberterrorism through the lens of its use by groups traditionally recognized as terrorist organizations, such as Al Qaeda or ISIS, for example.

Such examples of cyberterrorism—those with tangible impacts or ties to conventional terrorist organizations—must be noted in any assessment of this new form of terrorism. However, cyberterrorism's utility in disrupting intangibles like privacy, psychological security, or the trustworthiness of financial and government institutions, makes it an attractive tool for those who hope to sow fear and confusion in their targets.

So what makes cyberspace such an appealing threat vector for a new generation of terrorists? At the most basic level, the ability to instantaneously obtain a desired nefarious end state across the world without the same trail of evidentiary "breadcrumbs" typically associated with conventional acts of terrorism is a highly desirable and inherent capability in terms of cyberterrorism.[10] The ability to remain anonymous, or to simply complicate attribution of an attacker's true identity or intention, is a key component to cyber attacks – and one that adds to the psychological effect of an attack. Even though this has made cyber attacks more appealing and prevalent, the concept of cyberterrorism has not generated a larger body of evidence of its impacts on individuals' psychology or perceptions. In lieu of this, there is evidence of the psychological impact of online harassment (or "cyber bullying"), which should be considered an important indicator of

[9] Vytautas Butrimas, "National Security and International Policy Challenges in a Post Stuxnet World," *Lithuanian Annual Strategic Review* 12, no. 1 (2013).
[10] Rogers, "The Psychology of Cyber-Terrorism."

things to come in terms of future acts of cyberterrorism as these "can have profound real-world consequences, ranging from mental or emotional stress to reputational damage or even fear for one's personal safety".[11] Cyber attacks and general acts of cyber "aggression" have been studied in greater detail and have shown a measurable and correlated impact on citizens' psychological mindset as well as influencing how they go about their daily lives.[12]

In light of recent high profile United States government institution compromises, such as the Office of Personnel Management or the tampering of the 2016 elections, as well as other large institutions with immediate impact to citizens, like Equifax, Americans have expressed a general lack of trust in the abilities of current institutions to protect them or their personal data from online predators.[13] [14] Unfortunately, this lack of trust is compounded by three key factors: the general lack of knowledge Americans have when it comes to cybersecurity, the overwhelming lack of trust Americans have in the United States government, and a disproportionate amount of attention given by major media outlets. In the absence of primary research on these three factors, this paper will leverage available data—in the form of significant secondary research and literature exists that examines these aspects separately—to attempt to address them and answer this paper's core research question.

2.1 Cybersecurity Knowledge

Studies have hinted at a possible generational gap in general cybersecurity knowledge, with younger generations typically having greater knowledge than older

[11] Maeve Duggan, "Online Harassment 2017," (Pew Research Center, 2017).
[12] Gross, Canetti, and Vashdi, "The Psychological Effects of Cyber Terrorism."
[13] Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," (Pew Research Center, 2017).
[14] Lee Rainie et al., "Anonymity, Privacy, and Security Online," (Pew Research Center, 2013).

generations. However, stronger ties were found between educational attainment and level of cybersecurity knowledge, with those that had higher levels of education had significantly more cybersecurity knowledge than those with lower levels of education.[15] Notably, these studies were conducted via telephonic surveys which could preclude some portions of the American population and do not appear to account for other potential variables that may have an impact on an individual's cybersecurity knowledge, such as occupation, employment status, or income, which this study intends to address.

2.2 Trust in Government

While social researchers often disagree on a common view of trust in one's government, it is important to understand the potential implications of governmental distrust and cyberterrorism. Among Americans, the public's trust in the American government to generally "do the right thing" has not risen above 30% since 1958, and when polled in October 2015, was at a near-historic low of 19%.[16] By living in a constant state of distrust, it is possible that citizens may be more likely to feel the effects of an act of terrorism, particularly if it were to occur via a cyber medium, an arena where most Americans have little advanced insight beyond general media portrayal.

2.3 Media Coverage

Like government credibility, the media is not without heavy criticism among researchers. Historical acts of more traditional forms of terrorism have long benefited from the copious amounts of media coverage they receive, with many researchers

[15] Kenneth Olmstead and Aaron Smith, "What the Public Knows About Cybersecurity," (Pew Research Center, 2017).
[16] Carroll Doherty et al., "Public Trust in Government Remains near Historic Lows as Partisan Attitudes Shift," (Pew Research Center, 2017).

blaming media outlets for rises in given acts of terrorism.[17] While an act of terrorism is obviously felt by the immediate surroundings of its epicenter, the media expedites its worldwide coverage. As mentioned earlier, this is no different for acts of cyberterrorism, after which media outlets would likely stream a continuous loop of coverage for days to weeks on end, further exacerbated by the novelty of the cyber medium that would be used.[18]

3. Data and Methods

3.1 Case Selection

This research focuses on the United States and cyber security for several reasons. Cyber attacks targeting critical infrastructure – once thought to be impractical and unfeasible – have become a reality, most recently demonstrated in the attacks on the Ukrainian power grid.[19] In these cases, an entire nation could be thrown into chaos by a single cyber threat actor, significantly more catastrophic compared to more conventional notions of terrorism whose initial impact is in an immediate area. Loss of power, water, or other critical infrastructure for a prolonged period could result in the deaths of thousands. Cyberterrorism is a threat that can span the globe without requiring any radicalization or support elements.

The United States has increasingly been targeted by cyber attacks – both by nation states and low-level hackers. In a recent release, The United States government has formally blamed Russia for hacking into the United States power grid. Russia, a

[17] Rogers, "The Psychology of Cyber-Terrorism."
[18] Ibid.
[19] "Alert (Ir-Alert-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure," ed. Industrial Control Systems Cyber Emergency Response Team (2016).

formidable cyber adversary and tied to previous attacks on the Ukrainian power grid, possesses the skills and equipment to launch nation-crippling cyberterrorism campaigns. Now more than ever, the United States needs to assess the potential impact of cyberterrorism.[20]

3.2 Dataset Description

As this research seeks to analyze the potential impact of cyberterrorism on American citizens' trust in the government, it uses a cross-sectional dataset obtained from Pew following telephonic surveys conducted in 2016 among a random national sample of 1,040 adults 18 years of age and older, spanning across all 50 states and Washington, D.C.[21]

3.3 Variable Description

For the purpose of this analysis, there are two dependent variables measured: trust in the United States government's ability to respond to a cyber attack on government entities and trust in its ability to respond to a cyber attack on public infrastructure. Both dependent variables take the values of "0" if respondents do not believe that the government is able to respond, "1" if respondents believe that the government is able to respond, and "2" if the respondent did not know if the government could respond, or refused to answer.

The independent variables used in analysis are age, sex, political party affiliation, political ideology, employment status, education level, whether the respondent has a

[20] "Alert (Ta18-074a): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," ed. United States Computer Emergency Readiness Team (2018).
[21] Olmstead and Smith, "Americans and Cybersecurity."

child, and whether or not they are a parent. Distinction is drawn between these last two variables as one can have a child, but not necessarily have an active parental role. Full descriptive statistics for the independent variables used can be found in Appendix Table 1 in Appendix A.

3.4 Method

Ordered logistic regression was used for analysis of the dependent variables.

4. Results

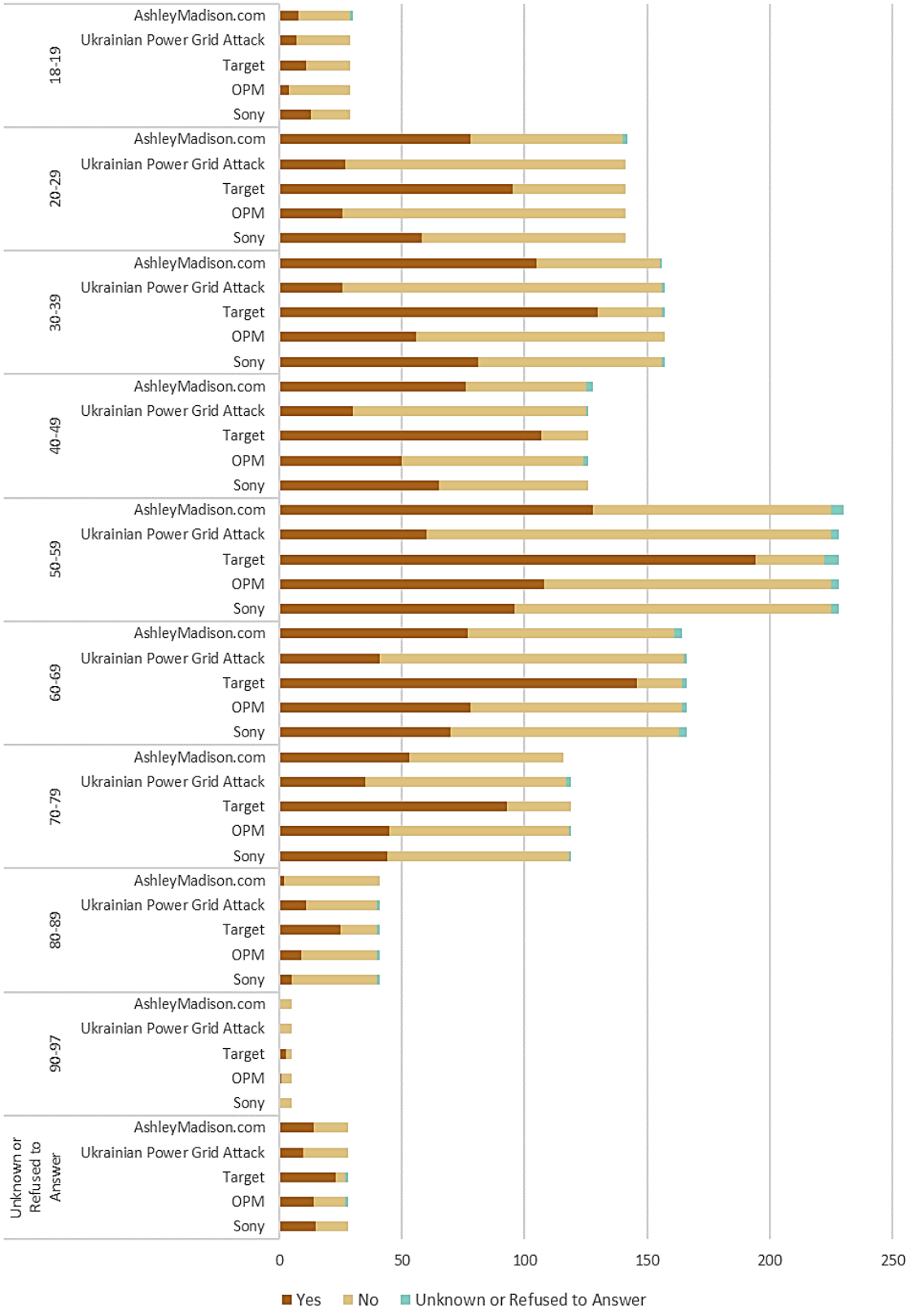
Survey results published by the Pew Research Center suggest that Americans generally lack trust in the United States Federal Government's ability to respond to cyber attacks.[22] However, analysis of the data suggests that United States citizens believe that the government is prepared to respond to attacks on both public infrastructure, as well as on its own federal agencies. Furthermore, analysis of the Pew data illuminates potentially significant factors that may impact overall trust levels.

Highly publicized cyber events covered extensively by mainstream media provide some measure of general cyber situational awareness of United States citizens. Figure 1 below depicts five recent major cyber security events and the age ranges of survey respondents who indicated whether they were aware of those events or not.[23] Respondents in each age cohort reported higher levels of awareness of cyber attacks that would most likely have had an impact on them directly, specifically AshleyMadison.com, Target, and Sony. It is quite possible that these individuals heard of these compromises as

[22] Ibid.
[23] Respondents were asked whether they had or had not heard of the following cyber attacks: Sony (2014), Office of Personnel Management (2015), Target (2013), Ukrainian power grid (2015), and AshleyMadison.com (2015).

part of the notifications sent to affected parties rather than through a news source. Interestingly, while the Office of Personnel Management compromise was a significant impact to personnel affiliated with the United States government, the frequency of those reporting awareness of the event were relatively low. This could be due in part that those affected were part of a specific subset of the population that had worked or currently work for the United States government in some capacity. The cyber attack on the Ukrainian power grid also drew a low awareness frequency, likely due to several factors, including lack of immediate threat or impact to respondents.

Figure 1: Cyber Event Awareness by Age Group



Age and general cyber security awareness are able to provide some means to anticipate reactions cyberterrorism. However, trust and feelings of security provided a more robust means of analysis. Table 2 shows a simple cross-tabulation concerning respondents' general trust of others and the security of their personal information online now compared with five years ago. 56.88 percent of those surveyed felt their personal information was less secure at the time of their response compared to five years prior and did not trust others, 17.98 percentage points more than those that felt less secure but trusted others. Interestingly, 52.53 percent of those that reported feeling that their personal information was as or more secure also reported that they generally did not trust others. While the percentage point difference between general trust and those reported to have felt as or more secure was less than those responding as feeling less secure, there was still a difference of 10.71 percentage points, suggesting that people in general do not trust others, regardless of how secure they may feel.

Table 1: Respondents' General Trust and Sense of Security Compared to Five Years Ago

	Online Security		
General Trust of Others	**Less Secure**	**As or More Secure**	***Total***
Do Not Trust	310 56.88	260 52.53	*570* *54.81*
Trust	212 38.90	207 41.82	*419* *40.29*
Unknown or Refused to Answer	23 4.22	28 5.66	*51* *4.90*
Total	*545* *100.00*	*495* *100.00*	*1,040* *100.00*

Key
Frequency
Column Percentage

To compare respondents' trust in the government's ability to respond to cyber attacks on both government entities as well as public infrastructure, similar cross-tabulation tables were used and the results for each are annotated in Table 3 and Table 4 respectively. These findings contradict Pew results that most of those surveyed lack trust in the government's ability to respond appropriately to an attack on a government entity

as well as an attack on public infrastructure, an interesting result considering the overwhelming majority feeling that their online security is less secure at the time of survey compared to five years prior.

Table 3: Respondents' Trust in Government and Sense of Security Compared to Five Years Ago: Response to Attacks on Government Entities

	Online Security		
Trust in Response: Government Entity	**Less Secure**	**As or More Secure**	***Total***
Do Not Trust	187 34.31	114 23.03	*301* *28.94*
Trust	339 62.2	364 73.54	*703* *67.6*
Unknown or Refused to Answer	19 3.49	17 3.43	*36* *3.46*
Total	*545* *100.00*	*495* *100.00*	*1,040* *100.00*

Key
Frequency
Column Percentage

Table 4: Respondents' Trust in Government and Sense of Security Compared to Five Years Ago: Response to Attacks on Public Infrastructure

	Online Security		
Trust in Response: Public Infrastructure	**Less Secure**	**As or More Secure**	***Total***
Do Not Trust	218 40.00	142 28.69	*360* *34.62*
Trust	303 55.6	335 67.68	*638* *61.35*
Unknown or Refused to Answer	24 4.4	18 3.64	*42* *4.04*
Total	*545* *100.00*	*495* *100.00*	*1,040* *100.00*

Key
Frequency
Column Percentage

Building on the concept of trust from Tables 2 through 4 above, additional analysis was conducted on the notion of trust in government response to cyber attacks through ordered logistic regression to determine what, if any, other independent variables may influence trust at an individual level, and could more accurately describe the results seen in the originating study, as well as possibly predict citizens' response to future cyber threats. Key independent variables were respondents' age, sex, political party affiliation, political ideology, education level, employment status, and if the respondent had a child

(summary statistics and additional information of the independent variables used in this research can be referenced in Appendix A). Table 3 provides the results of the ordered logistic regression on the dependent variable of trust in the government's ability to respond to a cyber attack on government agencies. In this model, respondent sex, political ideology, and education level are all significant. A one-point increase in respondents' sex – that is, going from female to male – is associated with a .24 percentage point drop in trust in government response to a cyber attack on a government entity. Interestingly, while political ideology is significant, party affiliation is not. This may be the result of individual beliefs driving perception versus simply being affiliated with a party where one may not agree with all its views. Ideological findings suggest that going from identifying as conservative to liberal is associated with a .16 percentage point decrease in trust, a result not expected considering the government was controlled by the Democratic party during the time of the survey. Lastly, an increase in education is associated with a .16 percentage point increase in trust.

Table 3: Ordered Logistic Regression of Variables on Citizen Trust in Government Response to Attacks on Government Entities

Variable	Coef. (Robust St. Error)
Age	.13 (.03)
Sex	-.24*** (.12)
Party Affiliation	.03 (.04)
Political Ideology	-.10* (.07)
Education	.16** (.09)
Employment Status	-.27 (.08)
Is a Parent	-.06 (.25)
Has a Child	-.11 (.25)
N	1,040
Model Fit Wald Chi-Square	 61.06

Note: Robust standard errors are given in parentheses under the estimated coefficients. * p < .1, ** p < .05, *** p < .01

Like Table 3 above, Table 4 below similarly analyzes trust in the government, but specifically trust in the government's ability to respond to a cyber attack on public infrastructure. Political ideology and education are significant in both tables, with age and employment status being statistically significant in Table 4. Like Table 3, political ideology is significant while party affiliation is not. Unlike Table 3, there is a negative relationship seen in the effect of education on overall trust in the government's ability to respond to a cyber attack on public infrastructure. As a respondent's educational attainment increases, their overall level of trust decreases by .12 percentage points. Additionally, going from unemployed to employed results in a .26 percentage point decrease in government trust.

Table 4: Ordered Logistic Regression of Variables on Citizen Trust in Government Response to Attacks on Public Infrastructure

Variable	Coef. (Robust St. Error)
Age	.045* (.03)
Sex	-.09 (.11)
Party Affiliation	-04 (.04)
Political Ideology	-.14*** (.07)
Education	-.19*** (.08)
Employment Status	-.26*** (.09)
Is a Parent	.01 (.25)
Has a Child	-.14 (.24)
N	1,040
Model Fit	
Wald Chi-Square	29.24

Note: Robust standard errors are given in parentheses under the estimated coefficients. * p < .1, *** p < .01

5. Conclusion

This research found that most of the originating sample of survey respondents felt they generally could not trust others and believed that their personal information was more vulnerable now than ever before. Despite this, the majority of those surveyed still had trust that the United States government would be able to respond and address a cyber attack on both government entities and public infrastructure, contradicting the results presented by Pew.

However, this research does have its limitations. First, the original Pew data lacks a question that addresses the method in which respondents became aware of mainstream cyber-related events, as well as if any additional research was conducted by the respondent following learning of a cyber attack. Determining these would provide not

only an additional measure of cyber awareness, but also the most influential mediums which could identify and scope future information warfare campaigns by threat actors. Second, this study evaluates more common forms of cyber attacks rather than acts of cyberterrorism, two different events. Future studies should attempt to evaluate responses to recent catastrophic cyber-related events, such as Stuxnet and the Ukrainian power grid attack and whether respondents still felt that they could trust the United States government to either mitigate or adequately respond. Interweaving of the psychological impact of cyberbullying or general cyber aggression should also be considered when conducting future research as the psychological impact may be similar to what could reasonably be expected to be observed following an act of cyberterrorism.

6. References

"Alert (IR-Alert-H-16-056-01): Cyber-Attack against Ukrainian Critical Infrastructure." edited by Industrial Control Systems Cyber Emergency Response Team, 2016.

"Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." edited by United States Computer Emergency Readiness Team, 2018.

"Annex of Statistical Information: Country Reports on Terrorism 2016 ". (2017).

Butrimas, Vytautas. "National Security and International Policy Challenges in a Post Stuxnet World." *Lithuanian Annual Strategic Review* 12, no. 1 (01//2013/2014 2013): 11-31.

Chen, Thomas M., and Lee Jarvis. *Cyberterrorism: Understanding, Assessment, and Response.* Edited by Thomas M. Chen, Lee Jarvis and Stuart Macdonald. New York: Springer, 2014. doi:10.1007/978-1-4939-0962-9.

"Country Reports on Terrorism." United States Department of Justice, Multiple.

Doherty, Carroll, Jocelyn Kiley, Alec Tyson, Bradley Jones, Baxter Oliphant, Rob Suls, Hannah Fingerhut, *et al.* "Public Trust in Government Remains near Historic Lows as Partisan Attitudes Shift." Pew Research Center, 2017.

Duggan, Maeve. "Online Harassment 2017." Pew Research Center, 2017.

"Final Report of the National Commission on Terrorist Attacks Upon the United States." Washington, District of Columbia: National Commission on Terrorist Attacks Upon the United States, 2004.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. "The Psychological Effects of Cyber Terrorism." *Bulletin of the Atomic Scientists* 72, no. 5 (2016/09/02 2016): 284-91.

Levav, Itzhak. "Terrorism and Its Effects on Mental Health." *World Psychology* 5, no. 1 (February 2006 2006): 35-36.

Olmstead, Kenneth, and Aaron Smith. "Americans and Cybersecurity." Pew Research Center, 2017.

———. "What the Public Knows About Cybersecurity." Pew Research Center, 2017.

Rainie, Lee, Sara Kiesler, Ruogu Kang, and Mary Madden. "Anonymity, Privacy, and Security Online." Pew Research Center, 2013.

Rogers, Marc. "The Psychology of Cyber-Terrorism." Chap. 4 In *Terrorists, Victims, and Society : Psychological Perspectives on Terrorism and Its Consequences*, edited by Andrew Silke. Wiley Series in the Psychology of Crime, Policing and Law, 77-92. Chichester, West Sussex, England: Wiley, 2003.

7. Appendix A: Independent Variable Definitions and Summary Statistics

Definitions and summary statistics are provided for the independent variables used in this research are outlined in Appendix Table 1 below.

Appendix Table 1: Independent Variable Definitions and Summary Statistics

Variable Name	Measure	Mean	Standard Deviation	Min	Max
age	Age *1 = 18-19* *2 = 20-29* *3 = 30-39* *4 = 40-49* *5 = 50-59* *6 = 60-69* *7 = 70-79* *8 = 80-89* *9 = 90-97* *10 = Unknown* *11 = Refused*	4.75	2.08	1	11
sex	Sex *0 = Female* *1 = Male*	.49	.5	0	1
party	Political party affiliation *1 = Republican* *2 = Democrat* *3 = Independent* *4 = No preference* *5 = Other*	2.35	1.05	1	5
ideo	Political ideology *0 = Conservative* *1 = Moderate* *2 = Liberal* *3 = Other*	1.05	.93	0	3
educ2	Highest level of education completed *1 = High School* *2 = College* *3 = Postgrad* *4 = Unknown* *5 = Refused*	1.95	.77	1	5
emplnw3	Employment status *0 = Unemployed or Other* *1 = Full Time* *2 = Part Time*	.76	.7	0	2
par	Is a parent *0 = No* *1 = Yes*	.27	.44	0	1
child	Has a child *0 = No* *1 = Yes*	.31	.46	0	1

8. Curriculum Vita

Michael Alan Sanders was born in San Antonio, Texas in August 1983. He is an M.S. Candidate in the Government Analytics program at Johns Hopkins University and received his B.A. in Sociology from the University of Pennsylvania. Michael's research interests include emerging cyber threats, asymmetric use of networked devices as attack mediums, and crime and recidivism in the United States.